Daily Open Source Infrastructure Report
6 April 2012

Top Stories

- A U.S. attorney in Las Vegas announced April 4 that 13 California residents were indicted in Nevada in an identity theft scheme that federal prosecutors said included placing card skimming devices on bank lobby doors. – *Associated Press* (See item **11**)
- The Utah Department of Health said tens of thousands of Medicaid claims records were accessed by Internet hackers. The files could include client names, birth dates, and Social Security numbers. – *KSL 5 Salt Lake City* (See item **23**)
- The Los Angeles Police Department radio communications were down for half the day April 3. The communications breakdown caused a delayed response to emergencies and prevented officers from gaining immediate access to information. – *Los Angeles Daily News* (See item **26**)
- More than 600,000 Macs were infected with a new version of the Flashback trojan installed on computers due to Java exploits, security researchers from antivirus vendor Doctor Web said April 4. – *IDG News Service* (See item **28**)
- Researchers released two new exploits that attack common design vulnerabilities in a computer component used to control critical infrastructure around the world, Wired reported April 5. – *Wired* (See item **29**)

Fast Jump Menu

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: LOW, Cyber: LOW
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - [http://www.esisac.com]

1. *April 5, Associated Press* – (West Virginia) **W.Va. coal mine where blast killed 29 to be sealed.** The West Virginia coal mine where an explosion killed 29 men 2 years ago April 5 will be permanently sealed with concrete, the mine's new owner said. Virginia-based Alpha Natural Resources, which acquired the mine when it bought Massey Energy in the summer 2011, said it will seal the portals, the large tunnels miners use to get underground, at the Upper Big Branch mine. Boreholes will be plugged and shafts that house the huge industrial fans meant to sweep bad air out of the mine will be capped to prevent any access. The job should be finished by the summer, the company said. An explosion fueled by methane and coal dust ripped through the seven miles of underground corridors at the former Massey Energy mine April 5, 2010.
Source: http://www.pantagraph.com/news/national/w-va-coal-mine-where-blast-killed-to-be-sealed/article_d830c4cd-bc52-51af-896c-8ac3253fa833.html

2. *April 5, Great Falls Tribune* – (Montana) **Texas company to revive Montana mine using CO2.** A Texas company said April 4 it is planning to revive production in a 45-year-old southeastern Montana oil field by pumping carbon dioxide deep underground to free up an estimated 30 million barrels of trapped crude. The Denbury Resources vice president said the $400 million Belle Creek carbon dioxide injection project is slated to begin operations by early 2013. The gas will be brought in by pipeline from a ConocoPhillips natural gas plant near Lost Cabin, Wyoming. A byproduct of natural gas production, carbon dioxide from such plants typically is vented into the atmosphere, contributing to the energy industry's greenhouse gas emissions.
Source:
http://www.greatfallstribune.com/article/20120405/NEWS01/204050302/Texas-company-revive-Montana-mine-using-CO2?odyssey=tab|topnews|text|Frontpage

3. *April 4, Kansas City Star* – (Kansas) **Fire breaks out at KCK power plant.** Kansas City, Kansas firefighters spent several hours April 4 battling a smoldering fire inside a coal chute at a power plant near the Missouri River. A spokesman for the Board of Public Utilities (BPU) said plant personnel extinguished the initial fire "relatively quickly." Firefighters on the scene throughout the afternoon reported they were continuing to use water and foam to completely extinguish the fire inside a chute used to feed coal from an upper storage bunker into boilers on a lower floor. Firefighters turned to foam after water proved ineffective. A BPU spokesman said the incident had no impact on any of its customers.
   Source: http://www.kansascity.com/2012/04/04/3536066/fire-breaks-out-at-kck-power-plant.html

For more stories, see items **15** and **29**

[Return to top]

Chemical Industry Sector

See item **29**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

4. *April 5, Associated Press* – (South Carolina) **Offsite power outage reported at SC nuclear plant.** Officials said crews were working to restore offsite power to the Catawba nuclear power plant near York, South Carolina, April 5. A news release said the U.S. Nuclear Regulatory Commission (NRC) was monitoring the situation at the plant. Officials said one of the two units at the plant was already shut down for an outage and the other unit automatically shut down after losing offsite power. The NRC said there was no impact to plant workers or the public. Officials will review the cause of the outage and determine if additional inspections are needed.
   Source: http://www.reflector.com/ap/staten/offsite-power-outage-reported-sc-nuclear-plant-1013925

5. *April 4, Associated Press* – (Nebraska) **Regulators: Fort Calhoun plant unlikely to open before fall.** Federal regulators said April 4 it was unlikely the Fort Calhoun nuclear power plant near Blair, Nebraska, will restart before the fall because of the extensive inspections and repairs needed. A Nuclear Regulatory Commission (NRC) official said he expects the agency will be conducting detailed inspections at Fort Calhoun through the summer. After that, NRC officials will review the situation before deciding whether the plant is ready to restart safely. Fort Calhoun has been shut down since planned refueling maintenance began in April 2011. Flooding along the Missouri River forced it to remain closed during the summer of that year.
   Source:
   http://www.wowt.com/news/headlines/Regulators_Fort_Calhoun_Plant_Unlikely_to_Open_Before_Fall_146213575.html?ref=575

[Return to top]

Critical Manufacturing Sector

See item 29

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

6. *April 5, Softpedia* – (International) **Fake BBB email helps fraudsters steal $100,000 from firm.** In December 2011, the Better Business Bureau (BBB) issued an alert regarding malicious e-mails purporting to originate from the BBB, urging recipients to download an alleged complaint that in reality contained malware. There are already a number of victims, one of which lost $100,000, Softpedia reported April 5. According to the Internet Crime Complaint Center, the agency received over 40 complaints, one of which from an organization that claims to have lost the large amount after the malware that came attached to the e-mail allowed the crooks to wire the money from the firm's bank account. It turns out that this was possible because of a keylogger that installed itself on the system when the attachment was opened and executed. The piece of malware recorded the company's banking password, giving the fraudsters the opportunity to transfer the money to their own accounts. Security experts found that some variants of the malicious notifications carry a link that redirects users to compromised WordPress sites that host the BlackHole Exploit Kit, which looks for vulnerabilities.
Source: http://news.softpedia.com/news/Fake-BBB-Email-Helps-Fraudsters-Steal-100-000-75-000-from-Firm-262950.shtml

7. *April 5, Greenwich Patch* – (Connecticut) **Two charged for ATM-skimming schemes in Greenwich & Stamford.** Two Romanian nationals were charged for their alleged roles in an ATM-skimming scheme based in Greenwich and Stamford, Connecticut, the U.S. attorney's office announced April 4. The pair were indicted March 19 but have been in custody in New York since August 14, 2011. The two entered not guilty pleas regarding the charges that they and other co-conspirators attached ATM skimming devices at three JP Morgan Chase Bank locations in Greenwich and Stamford. They also placed pinhole cameras at the locations to record users' personal information. The U.S. attorney's office alleges the defendants compromised approximately $72,000 from more than 100 customers. They both face charges of conspiracy, bank fraud, and aggravated identity theft.

Source: http://greenwich.patch.com/articles/two-charged-for-atm-skimming-schemes-in-greenwich-stamford

8. *April 4, Infosecurity* – (National) **IRS security dissing party continues.** The U.S. Internal Revenue Service's (IRS) Computer Security Incident Response Center (CSIRC), set up to monitor IRS networks, is failing to monitor 34 percent of the agency's servers, according to a Treasury audit, Infosecurity reported April 4. In the audit released March 2012, the Treasury Inspector General for Tax Administration (TIGTA) found that, in addition to not monitoring all of the IRS servers, the CSIRC was not reporting all computer security incidents to the Treasury as required. Also, IRS computer incident response policies, plans, and procedures "are either nonexistent or are inaccurate and incomplete." To remedy the center's shortcomings, the TIGTA recommended the IRS' assistant chief information officer for cybersecurity direct the CSIRC to develop its cybersecurity data warehouse capabilities to correlate and reconcile active servers connected to the IRS network with servers monitored by the host-based intrusion detection system; revise and expand the agreement with the TIGTA to ensure all reportable and relevant security incidents are shared with the CSIRC; collaborate with the TIGTA to create common identifiers to help the CSIRC reconcile its incident tracking system with TIGTA; develop a stand-alone incident response policy or update the policy in the IRS's manual with current and complete information; develop an incident response plan; and develop, update, and formalize all critical standard operating procedures.
   Source: http://www.infosecurity-magazine.com/view/24979/irs-security-dissing-party-continues/

9. *April 4, Reuters* – (New York; National) **CFTC orders JPMorgan to pay $20 million in Lehman case.** The U.S. Commodity Futures Trading Commission (CFTC) said April 4 that JPMorgan Chase & Co will pay $20 million to settle charges that it unlawfully handled customer segregated funds at Lehman Brothers Holdings Inc. The action comes as the CFTC and other regulators continue to probe what happened to segregated customer funds in the October 2011 collapse of MF Global Holdings Ltd, a commodity trading firm that also did business with JPMorgan. In the Lehman case, the CFTC said that for about 22 months, ending with Lehman's bankruptcy in September 2008, JPMorgan had improperly extended intra-day credit to Lehman Brothers based in part on customers' segregated funds Lehman had deposited at the bank. JPMorgan also violated rules by refusing to release customers' segregated funds for nearly 2 weeks after the bankruptcy, the CFTC said.
   Source: http://www.reuters.com/article/2012/04/04/us-jpmorgan-cftc-idUSBRE8330NM20120404

10. *April 4, South Florida Sun-Sentinel* – (Florida) **Broward woman pleads guilty in multimillion-dollar mortgage fraud.** A woman pleaded guilty April 4 to her role in two mortgage fraud schemes, worth about $12 million, in Florida's Broward and Palm Beach counties. She pleaded guilty to conspiring to commit wire fraud and four counts of wire fraud. She was the president of Direct Title & Escrow Services Inc. in Oakland Park. Prosecutors said she conspired with others to obtain high-value mortgages using fraudulent home loan applications and closing statements. Federal agents tracked her

down in Jamaica after the fraud was discovered.
Source: http://www.orlandosentinel.com/news/local/fl-mortgage-fraud-plea-wilks-20120404,0,5835085.story

11. *April 4, Associated Press* – (California; Nevada) **13 from Calif. indicted in Vegas ID skimming scam.** Thirteen California residents were indicted in Nevada in an identity theft scheme that federal prosecutors said included placing card skimming devices on bank lobby doors. A U.S. attorney in Las Vegas announced April 4 that 11 people were arrested in California on a sealed indictment handed up by a grand jury March 13. Two additional people were being sought. The defendants could each face 13 years in federal prison if convicted of conspiracy and aggravated identity theft charges. The indictment alleges that from November 2009 to November 2011 the co-conspirators captured ATM, credit card, and identity information from internal electronics of doors allowing after-hours access to ATM lobbies at Chase Bank branches. The scheme also allegedly involved using pinhole cameras to capture customer ATM personal identification numbers.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2012/04/04/state/n130200D16.DTL

12. *April 4, al.com* – (Alabama) **Investigators still looking for source of bank dye packs found near Tuscaloosa Amphitheater.** Authorities have not linked two bank dye packs found near the Tuscaloosa Amphitheater the week of March 26 to any known bank robberies, according to police in Tuscaloosa, Alabama. Investigators from the Tuscaloosa Police Department and FBI are looking into the source of the dye packs that were found March 29 on a path near the amphitheater, a police spokesman said. He added that no usable money or a bag was found with the dye packs, which are concealed explosive devices designed to mark stolen money with a bright dye. The dye packs will be sent to the manufacturer for safe deactivation, he said.
Source: http://blog.al.com/tuscaloosa/2012/04/investigators_still_looking_fo.html

[Return to top]

Transportation Sector

13. *April 5, New York Daily News* – (New York) **Water main break in lower Manhattan disrupts subway service on 1, 2 & 3 lines.** A 20-inch water main ruptured in the lower Manhattan area of New York City, early April 5, disrupting subway service, authorities said. The water main, which runs under West Broadway, broke between Chambers and Murray Streets, sending water surging up onto the street from a manhole and flooding subway tunnels with up to 4 feet of water, officials from the Department of Environmental Protection and Metropolitan Transportation Authority said. Service on the 1, 2, and 3 subway lines in lower Manhattan was suspended for several hours but had been partially restored almost 4 hours later. While the cause of the break is still under investigation, the age of the pipe was likely a factor.
Source: http://www.nydailynews.com/new-york/water-main-break-manhattan-disrupts-subway-service-1-2-amp-3-lines-article-1.1056489

14. *April 5, Associated Press* – (Texas) **Schneider National reopens hub.** Wisconsin-based Schneider National Inc. reopened its operating center near Dallas April 4, 1 day after a tornado swept through the area and sent several of the trucking company's trailers sailing through the air. Employees who took shelter in a building said the storm did not sound too bad, so they were "absolutely shocked" when they walked outside and saw the company's orange semis tipped over or left strewn along highways and parking lots, a Schneider spokeswoman said. About 65 people work at the facility, and 200 to 300 drivers visit the facility each day. She was not sure how many people were on site when the tornado touched down but said no one was injured and the building was largely untouched. There were about 250 trucks and 200 trailers on site when the twister hit. About 100 pieces of equipment sustained some level of damage. The National Weather Service said as many as a dozen twisters touched down April 3 in a wrecking-ball swath of violent weather that stretched across Dallas and Fort Worth. The storm left thousands without power and hundreds of homes pummeled.
Source:
http://www.postcrescent.com/article/20120405/APC0101/204050525/Schneider-National-reopens-Dallas-hub-after-tornadoes-story-videos-photos-

15. *April 5, Houston Chronicle* – (Texas) **Gas line break causes shelter-in-place at port, nearby industries.** Workers at the Port of Houston Authority's Jacinto Port terminal were told to shelter in place after a bulldozer at a nearby construction site hit a gas line April 5, a port spokeswoman said. The accident was not on port property but happened near the Jacinto Port Terminal on Jacinto Port Boulevard, said a spokeswoman. Harris County Sheriff's Office was managing the scene.
Source: http://fuelfix.com/blog/2012/04/05/gas-line-break-causes-shelter-in-place-at-port-nearby-industries/

For another story, see item **19**

[Return to top]

Postal and Shipping Sector

16. *April 4, WKSR 98.3 Loretto* – (Tennessee) **Two Loretto mailboxes vandalized.** Deputies with the Lawrence County, Tennessee Sheriff's Department were dispatched to a house in Loretto shortly after 10 p.m. March 30. The resident reported he had heard a loud, explosion-type noise outside his home. When he went outside to investigate, he said he discovered that his mailbox had been destroyed. Reports show that the mailbox was vandalized through use of some type of explosive device. Deputies found metal fragments from the device lying around the area, and reported detecting a strong odor of gun powder. He told deputies that he noticed a red truck driving past his home several times directly after the incident. Deputies were dispatched March 31 to investigate a similar incident at a home in Loretto. The resident reported his mailbox had been destroyed sometime overnight. Deputies note that the second vandalism appeared to have occurred as the result of an explosive device as well.
Source: http://www.wksr.com/wksr.php?rfc=src/article.html&id=30213

[Return to top]

Agriculture and Food Sector

17. *April 4, Food Safety News* – (International) **Tomme d'Or cheeses recalled in British Columbia.** The British Columbia Center for Disease Control (BCCDC) is warning the public not to eat Tomme d'Or cheese made by Moonstruck Organic Cheese on Saltspring Island because it may be contaminated with Listeria monocytogenes. Other types of cheeses produced by Moonstruck Organic Cheese are not affected by the advisory, according to the BCCDC April 4. Routine sampling by the BCCDC and further investigation by the cheese maker detected Listeria monocytogenes in the finished product. Affected products include all lot numbers of Moonstruck Tomme d'Or cheese, which sold at various retailers throughout British Columbia.
Source: http://www.foodsafetynews.com/2012/04/tomme-dor-cheeses-recalled-in-british-columbia/

18. *April 2, WFXS 55 Wausau* – (Wisconsin) **More than 70 cows die in overnight barn fire.** A barn more than a century old was destroyed by a April 1 fire in township of Rietbrock, Wisconsin. Dozens of milk cows were inside the building at the time and died in the fire. More than 70 of his cows were trapped inside the barn. Firefighters from around the area spent 4 hours putting out the fire.
Source: http://www.myfoxwausau.com/story/17316283/more-than-70-cows-die-in-overnight-barn-fire

[Return to top]

Water Sector

19. *April 5, Daily Hampshire Gazette* – (Massachusetts) **Easthampton water lines break; repairs snarl early-day traffic.** Two water lines in Easthampton, Massachusetts, broke in the city's center about 6 hours apart April 4. For the second time in a week, breaks due to aging equipment, sent water bubbling up into streets, and backed up traffic along Route 10 during rush hour. The Department of Public Works (DPW) attempted to shut a valve to stop the flow of water to the broken line causing another to "blow apart" due to the pressure. Road crews pumped water from a 5-foot-deep trench as police directed traffic. Crews finished and turned water back on 17 hours later. A city engineer estimated at least 200,000 gallons of water were lost as a result of the breaks. The DPW responded to another water main the week of March 26. The break occurred at the same time the fire department was battling a fire at an apartment building, and officials suspect the simultaneous incidents were probably related.
Source: http://www.gazettenet.com/2012/04/05/easthampton-water-lines-break-repairs-snarl-early-day-traffic

20. *April 4, Louisville Courier-Journal* – (Kentucky) **MSD spills sewage into Ohio River.** The Metropolitan Sewer District (MSD) reported a sewage spill of 2.5 million gallons into the Ohio River April 4. The spill was caused by an electrical failure at the agency's Starkey Pump Station in the Butchertown area of Louisville, Kentucky, a

senior MSD engineer said. He said the overflow was stopped about 2 hours after it was reported. The plant was opened in 2005 and handles most of the sewage from the Beargrass Creek watershed.
Source: http://www.courier-journal.com/article/20120404/NEWS01/304040101/MSD-spills-sewage-into-Ohio-River?odyssey=nav|head

21. *April 4, WBTV 3 Charlotte* – (North Carolina) **High levels of bacteria remain in park pond after sewage spill.** Charlotte-Mecklenburg, North Carolina officials said test results released April 4, show bacteria levels are three times the normal amount at the Park Road Park pond. A local resident discovered a sewage spill the week of March 26 but waited five days to report it to Mecklenburg County officials. Approximately 2,000 gallons of sewage spilled into a tributary that flows into the pond before a sewage pipe was fixed. A blockage of kitchen grease ruptured the sewage pipe, causing the spill. Charlotte-Mecklenburg Storm Water Services planned to test the water quality in the pond to determine the sewage spill's impact.
Source: http://www.wbtv.com/story/17324138/sewage-spill-may-have-leaked-into-park-road-park-city-says

22. *April 4, Arlington Heights Daily Herald* – (Illinois) **Elgin trying to identify yellow substance found in Tyler Creek.** Teams in Eglin, Illinois, were trying to identify a yellow substance found in Tyler Creek March 30 and again April 2. Crews spent hours probing storm sewers with video equipment to find a source for the substance but had no luck. The public works superintendent said the substance dilutes very quickly in the water. Crews were able to minimally test a diluted sample but came to no conclusions. The superintendent said his team is assuming it is relatively benign because of how quickly it dilutes in the water. The environmental concern is significant because Tyler Creek runs into the Fox River, where both Elgin and South Elgin pump water for public use. The Illinois Environmental Protection Agency was notified of the issue.
Source: http://www.dailyherald.com/article/20120404/news/704049696/

For more stories, see items **13** and **29**

[Return to top]

Public Health and Healthcare Sector

23. *April 4, KSL 5 Salt Lake City* – (Utah) **Hackers steal Utahns' personal medical info, 24,000 Medicaid files.** April 4, the Utah Department of Health (UDOH) advised Medicaid recipients to monitor their credit and financial accounts following a security breach of thousands of Medicaid claims records by Internet hackers. According to UDOH, the breach occurred March 30 as technicians from the Utah Department of Technology Services (DTS) were exchanging computer servers. Information from about 24,000 files stored on servers like the one that experienced the breach could include client names, addresses, birth dates, Social Security numbers, physician's names, national provider identifiers, addresses, tax identification numbers, and procedure codes designed for billing purposes. The DTS executive director said the newly installed server had "weaker controls" than the server it was exchanged for,

creating a system vulnerability. The affected server has been shut down, and new security measures have since been implemented. Initial tracing of the downloaded information pointed to Eastern Europe, but officials acknowledged the hackers could be working from elsewhere.
Source: http://www.ksl.com/?nid=148&sid=19861694

[Return to top]

Government Facilities Sector

24. *April 4, WCMH 4 Columbus* – (Ohio) **FBI interviews Olentangy High School student after bomb threat.** The FBI is interviewing a student at Olentangy High School in Lewis Center, Ohio, who allegedly made a bomb threat April 4. Sheriff's deputies and fire crews responded to the high school and called the Franklin County Bomb Squad. According to the sheriff's office, a freshman male student told another student not to come to school April 5 because a bomb would go off. Someone overheard the statement and called authorities. Officials said the student who allegedly made the threat is not from the United States and is scheduled to leave the country April 6. The FBI is interviewing the student who allegedly made the threat. The joint terrorism task force was called to investigate. All students were evacuated to the football stadium and were dismissed early due to the threat.
Source: http://www2.nbc4i.com/news/2012/apr/04/7/crews-investigate-threat-olentangy-high-school-ar-989090/

For more stories, see items **8**, **25**, and **35**

[Return to top]

Emergency Services Sector

25. *April 4, Ars Technica* – (Alabama; Texas; International) **Feds charge confessed Anon member after tracking his digital footprints.** April 4, Ars Technica reported that a Texas man was criminally charged with taking part in a string of hacks that targeted government and law-enforcement Web sites under the banner of "CabinCr3w," an offshoot to the Anonymous hacking collective. The Linux administrator from Galveston, Texas, was charged with unauthorized access to a protected computer, according to documents filed in U.S. District Court in Austin. His hacks, under a campaign his group took to calling "Operation Pig Roast," allegedly penetrated sites operated by at least four law-enforcement groups and in some cases dumped phone numbers, addresses, and other personal information belonging to police officers. He was also accused of hacking into the County of Houston's Web site in Alabama.
Source: http://arstechnica.com/business/news/2012/04/feds-charge-self-confessed-anonymous-member-after-tracking-his-digital-footprints.ars

26. *April 4, Los Angeles Daily News* – (California) **LAPD radio system fails for 12 hours.** The Los Angeles Police Department (LAPD) radio communications was down for half the day April 3. A city councilman said he will call for the dismissal of the

General Services Department general manager for the power outage at Mount Lee, where all LAPD radio communications equipment is housed. The city councilman said General Services crews were sent to the Mount Lee facility to test a backup generator. He said the test failed and knocked out all power at Mount Lee, shutting down radio communications, placing "the public and officers at extreme risk." LAPD officials and the Mayor's Office said backup systems were used that ultimately prevented any serious breakdowns in communication. According to the councilman, the communications breakdown meant a delayed response to emergencies, as 9-1-1 calls had to be answered manually with operators then calling stations to dispatch an officer. For officers, he said, the danger came in the form of an inability to get immediate access to information, such as a driver history based on license plates.
Source: http://www.dailynews.com/politics/ci_20329374/lapd-radio-system-fails-12-hours

27. *April 4, WAAY 31 Huntsville* – (Alabama) **Faulty radios put lives at risk.** The mobile radios used by Alabama's Madison County Sheriff's Department are unreliable at best and are putting deputies' lives at risk, WAAY 31 Huntsville reported April 4. Many times dispatch is unable to communicate with deputies while they are responding to calls. "We have basically devised a system where most of the officers also have cell phones and if we can't raise them for radio checks they automatically call their cell phones to see if they can get a check on them," explained a Madison County Sheriff's lieutenant. The lieutenant is on the department's radio board and says the current handhelds have a 20 percent chance of working once a deputy is inside a building. Another problem is that personnel cannot communicate with the Huntsville or Madison police departments. The FCC requires a change to a digital platform no later than January 1, 2013. However, this communication solution will present problems of its own when hundreds of people are trying to talk at the same time.
Source: http://www.waaytv.com/news/local/story/Faulty-Radios-put-Lives-at-Risk/dPHeROPUy0e2tbDMZ_Qf2A.cspx

For another story, see item **30**

[Return to top]

Information Technology Sector

28. *April 5, IDG News Service* – (International) **Fast-growing Flashback botnet includes over 600,000 Macs, experts say.** More than 600,000 Macs have been infected with a new version of the Flashback trojan being installed on people's computers with the help of Java exploits, security researchers from antivirus vendor Doctor Web said April 4. Flashback is a family of Mac OS malware that appeared in September 2011. Older Flashback versions relied on social engineering tricks to infect computers, but the latest variants are distributed via Java exploits that do not require user interaction. April 3, Apple released a Java update in order to address a critical vulnerability being exploited to infect Mac computers with Flashback. However, a large number of users have already been affected by those attacks, Doctor Web said in a report issued April 4. The company's researchers managed to hijack a part of the Flashback botnet through a

method known as sinkholing, and counted unique identifiers belonging to more than 550,000 Mac OS X systems infected with the trojan. Over 300,000 of the Flashback-infected Macs, or 56 percent of the total, are located in United States, while over 100,000 are located in Canada, Doctor Web said. The United Kingdom and Australia are next, with 68,000 and 32,000 infected Macs, respectively. The botnet is growing at a rapid rate. Hours after Doctor Web issued its report, one of the company's malware analysts announced the botnet had grown to over 600,000 infected computers. He also said 274 Macs infected with the new Flashback variant were located in Cupertino, the U.S. city where Apple has its headquarters.
Source:
http://www.computerworld.com/s/article/9225862/Fast_growing_Flashback_botnet_includes_over_600_000_Macs_experts_say?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&ut

29. *April 5, Wired* – (International) **Researchers release new exploits to hijack critical infrastructure.** Researchers released two new exploits that attack common design vulnerabilities in a computer component used to control critical infrastructure. The exploits attack the Modicon Quantum programmable logic controller (PLC) made by Schneider-Electric, which is a key component used to control functions in critical infrastructures around the world, including manufacturing facilities, water and wastewater management plants, oil and gas refineries and pipelines, and chemical production plants. One of the exploits allows an attacker to send a "stop" command to the PLC. The other exploit replaces the ladder logic in a Modicon Quantum PLC so that an attacker can take control of the PLC. The exploits take advantage of the fact that the Modicon Quantum PLC does not require a computer that is communicating with it to authenticate itself or any commands it sends to the PLC — essentially trusting any computer that can communicate with the PLC. Without such protection, an unauthorized party with network access can send the device malicious commands to seize control of it, or simply send a "stop" command to halt the system from operating. The attack code was created by an industrial control systems security researcher with Digital Bond, a computer security consultancy that specializes in the security of industrial control systems. The company said it released the exploits to demonstrate to owners and operators of critical infrastructures that "they need to demand secure PLC's from vendors and develop a near-term plan to upgrade or replace their PLCs." The exploits were released as modules in Metasploit, a penetration testing tool owned by Rapid 7 that is used by computer security professionals to quickly and easily test their networks for specific security holes that could make them vulnerable to attack. The exploits were designed to demonstrate the "ease of compromise and potential catastrophic impact" of vulnerabilities and make it possible for owners and operators of critical infrastructure to "see and know beyond any doubt the fragility and insecurity of these devices," said Digital Bond's CEO.
Source: http://www.wired.com/threatlevel/2012/04/exploit-for-quantum-plc/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+wired/index+(Wired:+Index+3+(Top+Stories+2))&utm_content=Google+Reader

30. *April 5, The Register* – (International) **Fake cop trojan 'detects offensive materials' on PCs, demands money.** Security firms are warning about a rash of police-themed ransomware attacks. The Reveton trojan warns victims illegal content has supposedly been detected on infected machines, displaying a message supposedly from local police agencies demanding payment to unlock machines. To unlock an infected machine, victims are asked to purchase an unlock code. However, control of infected machines can be re-established for free by following a series steps, as outlined by both F-Secure and Microsoft. Trend Micro believes some of the criminals peddling the Reveton trojan were also involved in the high-profile DNSChanger trojan scam, the target of a successful Microsoft takedown operation in November 2011.
Source: http://www.theregister.co.uk/2012/04/05/police_themed_ransomware/

31. *April 5, Softpedia* – (International) **ABB refuses to patch vulnerabilities in legacy systems.** A pair of researchers identified a buffer overflow flaw in a number of components of the ABB WebWare Server applications that are currently being used in many legacy ABB products. However, because the products are approaching the end of their life cycle, the company said no patches should be expected. According to an Industrial Control Systems Cyber Emergency Response Team advisory, there are still some industrial control systems which rely on products such as ABB's WebWare Server SDK, ABB Interlink Module, S4 OPC Server, QuickTeach, and RobotStudio Lite. As the researchers highlight, some of the COM and ActiveX components inside them present vulnerabilities in the COM and scripting interfaces. The products are designed to facilitate communications with the robot controller, some provide graphical elements for Web pages, and others are used for human-machine interfaces. If the vulnerabilities from these products were to be exploited successfully, an attacker could cause a denial-of-service state for the application and even execute his/her own malicious code. For the time being, there are no known exploits that target the flaws in the aforementioned components, but developing one requires only a medium skill level.
Source: http://news.softpedia.com/news/ABB-Refuses-to-Patch-Vulnerabilities-in-Legacy-Systems-263008.shtml

32. *April 4, SecurityNewsDaily* – (International) **Updated Android malware can take over your phone.** A customized variant of Android malware is now worming its way onto nonrooted devices and taking them over, and the weapon requires no interaction from the victim to begin its campaign. Researchers at the mobile security firm Lookout identified the reworked malware as Legacy Native (LeNa), which poses as a legitimate app to gain unauthorized privileges on Android phones. LeNa has long plagued Android users, Lookout said, but in its reworked form, it no longer requires its target phone to be rooted, and can now activate its payload — it connects to remote servers, transmits sensitive phone information, and drops more rigged software onto the phone — without any complicity from the end user. The new Android malware disguises itself in fully functional copies of apps, including "Angry Birds Space," and hides its malicious payload in the string of code at the end of an otherwise genuine JPEG file, Lookout said. This rogue code exploits the GingerBreak vulnerability, a flaw that enables it to gain control of the phone and trick the victim into purchasing apps from illegitimate app stores.
Source: http://www.securitynewsdaily.com/1692-android-malware-legacy-native.html

For more stories, see items **6** and **8**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: https://www.it-isac.org

[Return to top]

Communications Sector

33. *April 5, Lincoln Courier* – (Illinois) **WLLM programs are back on the air.** WLLM 1370 AM and 105.3 FM Lincoln, Illinois, announced April 4 the majority of their national and local programs, music, and news were back on the air. An electrical fire March 12 forced station employees to evacuate their building, which interrupted their broadcasting. Music resumed March 19, but other programming was only reinstated the week of April 2. Live programs, such as local church services and the Record Request Show, will return to the air after WLLM has moved back into its building. Station directors are hopeful that normal operations will resume in the next 2 to 3 weeks. Source: http://www.lincolncourier.com/topstories/x586051089/WLLM-programs-are-back-on-the-air

34. *April 4, WTOV 9 Steubenville* – (Ohio) **Phone lines stolen again, residents without service.** For the third time in the last several months, someone cut phone lines in Jefferson County, Ohio, to try and take the copper, WTOV 9 Steubenville reported April 4. Police said the lines were cut along along Tweed Avenue early April 4 leaving several homes without service. The Jefferson County sheriff said the thief took about 300 feet of wiring and left about another 200 feet along the road. The lines belong to AT&T, who had crews on scene working to repair the outage. The sheriff said they have a lead on a suspect. As for a restoration time, AT&T had not given one. Source: http://www.wtov9.com/news/news/local/phone-lines-stolen-again-residents-without-service/nMKFn/

[Return to top]

Commercial Facilities Sector

35. *April 5, Lebanon Daily News* – (Pennsylvania) **Woman charged in Calvary Chapel arson.** A Lebanon County, Pennsylvania woman was charged with two counts of arson in connection with the March 2 morning fire at Calvary Chapel in Lebanon. The fire was determined to have been deliberately set to the rear of the building based on an investigation conducted by the Lebanon City Bureau of Fire, the Lebanon Police Department, and the Bureau of Alcohol, Tobacco, Firearms and Explosives. Nearly 40 firefighters from 9 companies were on the scene for more than 6 hours battling the fire, which caused at least $100,000 damage. The Lebanon School District leases space

from the church for the Willow Street Academy. Classes were canceled at the building, but will resume there April 16.
Source: http://www.ldnews.com/ci_20322496/woman-charged-calvary-chapel-arson?source=most_viewed

For another story, see item **12**

[Return to top]

National Monuments and Icons Sector

36. *April 5, Central Florida News 13* – (Florida) **Brush fires burn in 2 counties, mobile home destroyed.** Florida's dry season is not over just yet, and a pair of brush fires causing big problems in two counties is proof. One fire got too close to a neighborhood in Volusia County, and another fast-moving fire threatened homes in Lake County, Central Florida News 13 reported April 5. A fire burned about 150 acres, including a home, April 4 near New Smyrna Beach. At the fire's height, authorities told residents near the area of Oak Rim Lane and Shadow Walk Lane to evacuate their homes. The evacuation order was lifted. Ninety firefighters from 9 different agencies worked on the fire, and crews managed to get the fire about 90 percent contained. In Lake County, a fire was estimated at 30-acres and several homes were evacuated near Lake Mack Road. Officials said the fire was caused by a vehicle fire. A shed and three vehicles were lost in the fire, but no homes were damaged. Florida Forest Service and Lake County Fire Department were working on the fire, and they said they hope the fire will burn itself out.
Source: http://www.cfnews13.com/content/news/cfnews13/news/article.html/content/news/articles/cfn/2012/4/4/crews_working_brush_

For another story, see item **38**

[Return to top]

Dams Sector

37. *April 5, Cape Girardeau Southeast Missourian* – (Louisiana) **USDA commits more money to fixing drainage in floodway.** Mississippi County, Missouri, will receive another infusion of funding from the United States Department of Agriculture's (USDA) Emergency Watershed Protection Program to repair drainage ditches damaged after the Birds Point levee breach in 2011 the Cape Girardeau Southeast Missourian reported April 5. Work began March 2012 to dig out what was left behind when the U.S. Army Corps of Engineers blasted holes in the levee protecting the floodway in a move to relieve flood pressure elsewhere. Representatives of the USDA's Natural Resource Conservation Service (NRCS) and Mississippi County Consolidated Drainage District No. 1 signed an amendment April 4 to a cooperative agreement for flood recovery work doubling the number of repair sites from three to six for a total of $3 million. The amendment makes an additional $2.1 million available to remove

sediment and debris left behind by floodwaters from drainage channels and dispose of the excavated material. NRCS will spend $13.7 million to clean out 108 miles of drainage ditches in the Birds Point New Madrid Floodway, said a state conservationist with NRCS. Throughout the Bootheel area $35 million will be spent to clean out 900 miles of ditches. There are 73 projects, including 14 in the Birds Point New Madrid Floodway, that will be completed in southeast Missouri during 2012 through the Emergency Watershed Protection Program. Work is scheduled to be completed by October 2012.
Source: http://www.semissourian.com/story/1833484.html

38. *April 4, Longview Daily News* – (Washington) **Looming dike collapse threatens Cathlamet deer refuge.** A badly eroded dike that keeps the Columbia River in Washington from flooding about 2,000 acres of a reserve for endangered Columbian White-tailed deer is in imminent danger of collapse, the Longview Daily News reported April 4. According to officials, the flooding could set back decades of deer-recovery efforts and perhaps threaten State Route 4 near Cathlamet. The county's public works director said April 3 that there was a real "risk of a deep-seated mass failure which could suddenly cause the whole dike to simply slide away into the river." Over time, the river channel has deepened along a bend in the river and has "created a hole underneath the rock that was placed to protect the dike, causing the rock (rip rap) to slide away," he said. Although the shipping channel has been deepened near that location, it was unclear whether dredging was a factor in the erosion. In late March 2012, an engineer contracted by the U.S. Fish and Wildlife Service, which manages the deer refuge, told the U.S. Army Corps of Engineers and county that the fix would cost between $2.7 and $4.5 million dollars because the damage was so extensive.
Source: http://tdn.com/news/local/looming-dike-collapse-threatens-cathlamet-deer-refuge/article_03c92094-7eb8-11e1-97ce-001a4bcf887a.html

[Return to top]

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2267
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer